UNITED STATES DISTRICT COURT FOR THE EASTERN DISTRICT OF VIRGINIA

ALEXANDRIA DIVISION

ABDULKARDIR NUR,

Plaintiff,

v.

UNKNOWN CBP OFFICERS, et al.,

Defendants.

Case No. 1:22-cv-00169-AJT-JFA

District Judge Anthony J. Trenga

PLAINTIFF'S OPPOSITION TO THE GOVERNMENT'S MOTION TO DISMISS

Both the Government's Motion to Dismiss as well as this broader case ask two core questions. First, can border agents—without any reasonable suspicion at all—force American citizens to unlock their phones (including providing necessary passwords), punishing them if they fail to comply, and then download the entire contents of that phone? Second, to the extent reasonable suspicion may allow such conduct, does watchlist placement—when watchlist placement does not require any reasonable suspicion of any criminal activity at all, much less a particular border-related crime—automatically provide that reasonable suspicion?

The answers to those questions are obvious: No. The Fourth Circuit has already answered them in *Kolsuz* and *Aigebekaen*.

The Government, naturally, does not like the answers. So the Government here attempts to break its actions down into tiny little segments and irrelevant legalese, so that maybe a violation of the Constitution is not a violation of the Constitution when each component of the violation is separated out and looked at in isolation.

The Court should reject the Government's overformalistic attempt to avoid the consequences of its unconstitutional conduct. Even under the Government's own deconstruction of its actions, the Constitution does not condone the various steps the Government has segregated its unconstitutional border search policy into. But the Court need not even reach those issues. Instead, the Court should just examine Nur's claims as they exist, rather than as the Government wishes them to be.

BACKGROUND

Abdulkadir Nur is a 69-year-old American citizen living in northern Virginia. Complaint ¶ 1. He is Muslim and from Somalia, having been naturalized more than 15 years ago. *Id.* And yet, every single time he lands at Dulles International Airport or anywhere else from overseas, CBP officers detain him—often for several hours—and seize his electronic devices. *Id.*

The reason for this—the only reason—is that the Government has placed Nur on a secret government watchlist. Nur does not know why. Nor will the Government (who will not even confirm Nur is on a watchlist) tell him. So Nur is therefore left to speculate.

Is it because he is Muslim?

Is it because of his business or humanitarian work? Nur is the CEO of a water welling and drilling company in Somalia. Complaint ¶ 76. He has worked with humanitarian groups such as the Red Cross since 1997 delivering food and resources to impoverished communities in East Africa. *Id.*

Is it because he was a victim? In September 2008, while providing logistical support to a United Nations relief program, delivering food and other aid in areas of Somalia devastated by conflict, Nur's caravan was raided by local insurgents. Complaint ¶ 77. A United Nations

Monitor Group subsequently launched an investigation, with which Nur participated fully, that ultimately found no fault in his action. *Id.* The FBI and US Attorney's Office later investigated, insinuating that Nur was a target of the investigation. *Id.* at ¶ 78. But after Nur fully cooperated, the Government closed the investigation without any charges, no longer even interested in Nur's willingness to provide additional evidence showing Nur's innocence. *Id.* at ¶ 79.

Although the Government did not press charges for Nur's innocent conduct, it placed Nur on the federal terrorism watchlist. Complaint at ¶ 80. In order to be placed on the watchlist, the Government must reasonably suspect an individual of being a known or suspected terrorist. *Id.* at ¶ 23. More specifically, the Government "must rely upon articulable intelligence or information which, based on the totality of the circumstances and taken together with rational inferences from those facts, creates a reasonable suspicion that the individual is engaged, has been engaged, or intends to engage, in conduct constituting in preparation for, in aid or in furtherance of, or related to, terrorism and/or terrorist activities." *Id.* Despite the use of the words terrorism or terrorist, watchlist status does not require that the Government reasonably suspect an individual in engaging in any particular criminal activity or indeed any criminal activity at all. *Id.* at ¶ 108. Instead, the Government may consider individual's race, ethnicity, country of origin, religion, religious practices, languages spoken, family, associations, travel history, social media history, and other activities protected by the First Amendment, Fifth Amendment, Fourteenth Amendment. *Id.* at ¶ 24. Indeed, immediate relatives of listed persons can be put on the watchlist without any additional derogatory information. *Id.* at ¶ 29. Likewise, individuals are subject to watchlist placement if they are colleagues, fellow community members, or other associates of those on the watchlist. *Id.* at ¶ 30.

Among the many consequences of watchlist placement is being subject to secondary searches and seizures at the border. Complaint at ¶ 21. According to CBP policy, advanced searches—what the Fourth Circuit calls forensic searches—are permitted for most individuals only when "there is a "reasonable suspicion of activity in violation of the laws enforced or administered by CBP, or in which there is a national security concern, and with supervisory approval." CBP Policy (Defs.' Mot. to Dismiss Ex. 2) at § 5.1.4. But when someone like Nur is on the watchlist, the rules are different. For individuals like Nur, "presence of an individual on a government-operated and government-vetted terrorist watch list" constitutes sufficient reasonable suspicion in and of itself. *Id.*

Nur did not cross the border from 2010—when he was likely placed on the watchlist—to 2018. Complaint at ¶ 81. But every time since he began crossing the border in 2018, the Government has detained Nur for several hours, interrogated him, demanded his device passwords, and seized his electronic devices. *Id.* at ¶ 83. Until 2020, Nur complied with the demands for his passwords. *Id.* But at that point, he refused. The Government responded by, among other things, shoving him against the wall, performing additional, aggressive searches, taking away his shoes, intimidating and threatening him, extending his detention, and seizing his devices for weeks before returning them. *Id.* at ¶ 89.

In order to get this unconstitutional conduct to stop, Nur has brought this case.

ARGUMENT

I. The Government's Border Search Policy violates Nur's Fourth Amendment rights

The Government places people on the watchlist based on a modified and watered down "reasonable suspicion" test. Complaint ¶ 23. That test determines whether there is "a reasonable suspicion that the individual is engaged, has been engaged, or intends to engage,

in conduct constituting in preparation for, in aid or in furtherance of, or related to, terrorism and/or terrorist activities." *Id.* But as explained by this Court in *Mohamed v. Holder*, 995 F. Supp. 2d 520, 531 (E.D. Va. 2014), conduct that can constitute being "related to" or "in aid" of terrorism sufficient to place an individual on the watchlist "is not necessarily related to any unlawful conduct."

Yet, once the Government decides this person meets this "reasonable suspicion" of being suspected of something vaguely related to terrorism test, the Government—as a matter of policy—asserts that this establishes the "reasonable suspicion" that is required, under Fourth Amendment law, for electronic searches. CBP Policy at § 5.1.4. This is an unconstitutionally permissive standard, as the Fourth Circuit requires "reasonable suspicion" of "criminal activity." *U.S. v. Cortez*, 449 U.S. 411, 417 (1981); *see generally U.S. v. Aigebekaen*, 943 F.3d 713, 718 n.2 (4th Cir. 2019)[1]; *U.S. v. Kolsuz*, 890 F.3d 133 (4th Cir. 2018). Further, that criminal activity must be "ongoing or imminent." *U.S. v. Kolsuz*, 185 F. Supp. 3d 843, 859 (E.D. Va. 2016) (citing *Cortez*, 449 U.S. at 417) ("An investigatory stop must be justified by some objective manifestation that the person stopped is, or is about to be, engaged in criminal activity."). Placement on a watchlist does not satisfy this standard.

Searching the electronics of individuals on the watchlist, without more, is squarely evidentiary and intelligence-gathering; it is not a search for contraband or firearms that justifies a warrant exception at the border. *Kolsuz*, 890 F.3d at 143 (noting "the scope of a warrant exception should be defined by its justifications" and warning that a border warrant exception would not apply in a situation where "the government invokes the border exception on behalf

[1] The Government suggests (at 15 n.6) that the reasonable suspicion requirement in *Kolsuz* is dicta, but *Aigebekaen* makes it a holding.

of its generalized interest in law enforcement and combatting crime") (citations omitted). Indeed, watchlist status does nothing to indicate that an individual's relationships or affiliations are illegal in any way, or have any international component, or that any component of those relationships and affiliations would be related to anything that might be on Nur's phone. The CBP policy ignores all of this, and defines Nur's watchlist status alone as adequate suspicion; as a result, CBP can perform a forensic search of Nur's phone for any reason or no reason at all.

The Court need not reinvent the wheel here. This very same issue was decided by the District Court in *El Ali v. Barr*, 473 F. Supp. 3d 479 (D. Md. 2020). As that Court explained, "[m]ere membership in the database … cannot supply individualized reasonable articulable suspicion." *Id.* at 521. After all, "[w]hat constitutes conduct sufficiently 'related to' or 'in aid of terrorism' is not explained, but it is not difficult to imagine completely innocent conduct serving as the starting point for a string of subjective, speculative inferences that result in a person's inclusion on the No Fly List."[2] *Id.* (quoting *Mohamed*, 995 F. Supp. 2d at 532). "The [watchlist] cannot serve as a proxy for individualized reasonable suspicion that an individual plaintiff is engaging in—or intends to engage in—terrorist activity at all, let alone at the time of the search." *Id.* "Accordingly, for those Plaintiffs who have averred facts to make plausible that they had been subjected to a non-routine search of their devices, Defendants' motion is denied." *Id.* So too here.

The Government has a number of responses to this, but none of them hold any water.

The Government suggests (Defs.' Mot. to Dismiss at 6, 12) that Border agents might

[2] The No Fly List is a subset of the broader watchlist. The standard for inclusion on the broader watchlist is less strict, and therefore necessarily at least as amorphous, as the standard for inclusion on the No Fly List.

be actually taking into account other factors that provide reasonable suspicion. But that is not CBP's policy. Under CBP's policy, border agents may search Nur's phone regardless of whether they can show independent reasonable suspicion. CBP Policy at § 5.1.4. Nor does the policy merely allow border agents to take into account watchlist placement when determining whether reasonable suspicion exists. Rather, watchlist placement constitutes reasonable suspicion. Full stop. Further, there is no evidence that, when Nur's watchlist status is communicated to agents when he crosses the border, the agents are given any underlying information to allow them to make their own informed choice whether reasonable suspicion exists. Rather, as far as the current record is concerned, all the border agents have at their disposal when deciding to search Nur is his watchlist status. Which, the policy instructs, is all they need. Indeed, as one CBP agent communicated to Nur, "he was just doing his job and that the mandate to search in this manner came from the system and not the reasonable judgment any CBP agent." Complaint ¶ 92.

The Government also suggests (at 19-20) that because searches are not mandatory, Nur lacks standing to challenge the policy. This appears to be a broader part of an attempt by the Government to somehow break down Nur's claims into facial and as applied components. The Government then treats the CBP policy's use of permissive rather than mandatory language to suggest that watchlisted individuals cannot challenge the policy prospectively. CBP Policy at § 5.1.3. As a result, the Government supposes, Nur would have to wait until the Government predictably and repeatedly violates Nur's rights, and then sue after the fact for damages only.

But as the Government correctly notes (Defs.' Mot to Dismiss at 1 n.1), such after the fact challenges are impermissible under the Supreme Court's *Bivens* jurisprudence. In any

event, as *El Ali* explained succinctly, "[w]here as here, Plaintiffs aver a historic pattern of such violations during similar travel, the Court may plausibly infer that such infringements will continue in the future." 473 F. Supp. 3d at 519; *see also Elhady v. Kable*, 391 F. Supp. 3d 562, 575 (E.D. Va. 2019), *rev'd on other grounds*, 993 F.3d 208 (4th Cir. 2021); *Mohamed*, 266 F.Supp.3d at 875 ("Plaintiff's decision not to engage in international travel because of the difficulties he reasonably expects to encounter upon return to the United States is sufficient to demonstrate standing."). And regardless of the text of the policy, both Nur's experience of over 8 international trips, as well as what a CBP officer told Nur himself, these searches, as a practical matter, are mandatory rather than discretionary. *See* Complaint at ¶¶ 82-91, 93; *see also id.* ¶ 92 (CBP agent telling Nur "the mandate to search in this manner came from the system and not the reasonable judgment any CBP agent").

The Government separately postulates (Defs.' Mot. to Dismiss at 18-19) that maybe the searches of Nur's devices are not forensic searches at all, and so no reasonable suspicion is required in the first place. But this is wrong for two reasons.

First, the facts make clear that the searches that are taking place are substantially the same searches performed in *Kolsuz* and *Aigebekaen*. The allegations in this case are not that with the password in hand, the agents thumbed through his email seeing what they can find. Instead, the allegations are that the officers "took those devices out of the room, to copy, download, or upload data, and then returned them upon Mr. Nur's eventual release." Complaint ¶ 83. These are forensic searches. *See U.S. v. Oloyede,* 933 F.3d 302, 308 (4th Cir. 2019) ("Mojisola took the phone, entered her passcode, and handed the phone back to Agent Winkis, who then gave the unlocked phone to a forensic examiner for it to be searched."); *U.S. v. Cotterman,* 709 F.3d 952, 962 (9th Cir. 2013) ("Agent Owen had a laptop with forensic

software that he could have used to conduct an examination at the port of entry itself, although he testified it would have been a more time-consuming effort. To carry out the examination of Cotterman's laptop, Agent Owen used computer forensic software to copy the hard drive and then analyze it in its entirety, including data that ostensibly had been deleted.") Yes, the agents did not formally acknowledge that it was performing a forensic search. But the CBP policy forbids such an acknowledgement. CBP Policy at § 5.4.2.5.

And when Nur refused with demands to provide his passwords, "Officers still took the devices out of the room, and on multiple occasions, seized them completely, refusing to return them until an extended, forensic search could be conducted offsite days or weeks later." Complaint ¶ 84. The obvious implication of the allegations is that CBP agents do the forensic search permitted by the policy either way, but that the forensic search is more complicated when, in addition to downloading the contents from the phone, it also has to overcome passwords. *Cotterman*, 709 F.3d at 958-59 (explaining process of forensic search of computer is more time-consuming without password). And this conforms with the thought-out decision in *United States v. Kameldoss,* 2022 WL 1200776 at *10 n.9 (E.D.N.Y. 2022), which explained in detail what the advanced searches covered under the CBP policy are and why, exactly, the Fourth Circuit requires reasonable suspicion for them.

But even if this Court accepted that—with forced password in hand—the searches that took place were not "forensic" searches under CBP policy or some other definition of the word, it would still require reasonable suspicion under *Kolsuz* and *Aigebekaen*. Forensic searches require reasonable suspicion under *Aigebekaen* because they are "'a powerful tool' capable of not only revealing data that a user has intentionally saved on an electronic device, but also 'unlocking password-protected files, restoring deleted material, and retrieving images

viewed on websites.'" *Aigebekaen*, 943 F.3d at 718 n.2 (quoting *Cotterman*,709 F.3d at 957); *see also US v. Kameldoss,* 2022 WL 1200776, at *10 n.9 (comparing manual and forensic searches, and expressly referring to advanced searches under CBP policy as forensic). It is precisely because forensic searches overcome the password protections that indicate an expectation of privacy that the Fourth Circuit ruled reasonable suspicion is required for them. So by demanding Plaintiff provide a password, CBP turns the search into one that requires reasonable suspicion regardless of whether CBP then uses forensic software thereafter (which it does).[3]

Finally, the Government (at Defs.' Mot. to Dismiss at 9-10) makes arguments about "facial challenges," "as applied challenges," and policies beyond the CBP's electronic data policy as applied to people on the watchlist. These arguments all miss the point. Nur is challenging the current effective policy, which is that Nur's watchlist status alone constitutes reasonable suspicion for purposes of performing forensic searches of Nur's devices.

II. CBP demands that Nur provide his password violates the Fifth Amendment

In *U.S. v. Hubbell*, the Supreme Court found that required provisions of passwords violated the Fifth Amendment precisely because providing those passwords were testimonial in nature. 530 U.S. 27, 35-36 (2000); *see Matter of Residence in Oakland, California*, 354 F. Supp. 3d 1010, 1016 (N.D. Cal. 2019) (same for biometric information); *see generally In Re Search of white Google Pixel 3 XL cellphone in a black Incipio case,* 2019 WL 2082709, at *4 (D. Idaho May

[3] The Government states (at 21) that *Kolsuz*, 890 F.3d at 146 cited CBP's 2018 Directive favorably, noting with approval that under the policy, advanced searches 'may be only with reasonable suspicion of activity that violates the customs laws or in cases raising national security concerns.'" But the issue of whether the watchlist inclusion standard meets constitutional requirements was not at issue in *Kolsuz*. The Fourth Circuit in *Kolsuz* was merely citing favorably the Government's quasi-admission that heightened standards were necessary. *Id.* Nur squarely challenges that 2018 CBP directive because it makes a "watchlist" exception to the heightened requirements otherwise imposed.

8, 2019); *In re Application for a Search Warrant*, 236 F. Supp. 3d 1066, 1073 (N.D. Ill. 2017). So too here. The requirement that Nur provide his password data (whether to facilitate or avoid a forensic search) is testimonial and violates the Fifth Amendment to the extent providing those passwords is compelled.

So, the only real question for this Court is whether the access Nur is compelled to give—and punished when he is refused—is compulsory. "A statement is compelled when considering the totality of the circumstances, the free will of the person making the statement was overborne." *El Ali v. Barr*, 473 F. Supp. 3d 479, 522 (D. Md. 2020) (citing *United States v. Washington*, 431 U.S. 181, 188 (1977)) (cleaned up). "To determine whether a defendant's will has been overborne or his capacity for self-determination critically impaired, courts must consider the 'totality of the circumstances,' including the characteristics of the defendant, the setting of the interview, and the details of the interrogation." *United States v. Braxton*, 112 F.3d 777, 781 (4th Cir. 1997) (cleaned up), quoted by *El Ali*, 473 F. Supp. 3d at 522.

Nur alleged that the passwords were demanded during periods where Nur was detained. Complaint ¶¶ 82-83, 85-87, 89-93. No reasonable person would believe that cooperation with the government making demands (not requests) of a detained person at the border was merely requesting voluntary cooperation. Indeed, the Complaint alleged that refusal ran the risk of prolonging he detention, effectively punishing the failure to cooperate. *See id.* ¶ 83 ("Believing he had no choice but to comply and afraid his refusal would prolong his detention, Mr. Nur gave the passwords, including biometric scans, to the officers who took those devices out of the room, to copy, download, or upload data, and then returned them upon Mr. Nur's eventual release"); *see also id* ¶ 85 (Nur's failure to comply led to a prolonged detention of over five half hours, resulting in a missed connection). Refusal also led to the Government seizing

Nur's devices "completely, refusing to return them until an extended, forensic search could be conducted offsite days or weeks later." *Id.* ¶ 84.

> As the Court in *El Ali* explained, some Plaintiffs' demands for passwords in that case
>
> > arose under coercive circumstances such as being held at gunpoint, in handcuffs, or in separate interrogation rooms. These same plaintiffs were often subjected to lengthy detentions during which access to family or counsel was denied. Additionally, Defendants do not dispute that the purpose of the interrogations was to gather information regarding terrorist activities, so any such interview may be plausibly inferred as designed to elicit incriminatory statements. Thus, certain Plaintiffs allege sufficient facts to make plausible that their Fifth Amendment rights against compelled self-incrimination had been violated.

El Ali, 473 F. Supp. 3d at 522 (record citations removed). Again, same here. *See* Complaint ¶¶ 85 (separate interrogation room); 86 (same); 87 (same); 89 (same, also "shoved against the wall and aggressively searched, deprived of his shoes, intimidated, and threatened by officers" after refusing); 90 (same, also "officers again became aggressive in an attempt to intimidate Mr. Nur into acquiescing"); 91 (same); 92 (same); 93 (same, also "the agent promised the detention would be over quicker if Mr. Nur complied" and when Nur still refused, "he agent insisted, threatening to keep the devices if he did not hand over the passwords," ultimately detaining Nur for over two hours).

The Government argues ("First," at 22) that the "right against self-incrimination only applies when introduced against a criminal defendant at trial, not in civil cases such as this one." *See also id.* at 26 (Government "Third"). The analogy is wrong and so is the assertion.

The analogy is wrong because Nur is not asking this Court to exclude information from his phone for use in this case. Instead, Nur is asking the Court to force the Government to stop violating his rights, whether or not that information is used against him in some future, hypothetical case. The claim is wrong because the remedy for a Fifth Amendment violation is not just one of evidentiary admission. Rather, the right not only protects against the use of

unlawfully-received evidence but also protects against the Government from violating the right in the first instance. *See Lefkowitz v. Cunningham,* 431 U.S. 801, 804 (1977) (affirming injunction against policy violating Fifth Amendment); *see also U.S. v. Kirschner*, 823 F.Supp.2d 665, 669 (E.D. Mi. 2010) (quashing of password-demanding subpoena); *Pentlarge v. Murphy*, 541 F. Supp. 2d 421, 427 (D. Mass. 2008) (incarceree class stated cause of action for declaratory and injunctive relief against program that punished them for refusing to waive Fifth Amendment rights by denying incarcerees treatment).

The Government's arguments otherwise distinguish between claims of privilege where there is a fear of prosecution and claims where there is no fear of prosecution. Motion to Dismiss at 24 (citing, among others, *United States v. (Under Seal*), 794 F.2d 920, 924 (4th Cir. 1986)). When the Government has labeled Nur a suspected terrorist and is seeking information related to his supposed terrorist activities, any fear of prosecution requirement is met here. As the Government asserts (at 24), the privilege "can be asserted in noncriminal cases [] 'where the answers might incriminate [the suspect] in future criminal proceedings.'" MTD at 24 (citing *Chavez v. Martinez*, 538 U.S. 760, 770 (2003)). Likewise, the Government provides no support for any assertion that the Fifth Amendment only applies to testimony procured in the course of a criminal investigation or when there is a risk of criminal prosecution, as no such requirement exists. The Fifth Amendment instead applies to all government information gathering, from Congressional testimony to civil subpoenas.

Nor does *Chavez* support the Government's argument in any event. As the Sixth Circuit explained, *Chavez*—a case where plaintiff solely sought § 1983 damages—was a case of no harm, no foul. *Moody v. Michigan Gaming Control Bd.*, 790 F.3d 669, 675 (6th Cir. 2015). It does not apply where, as here, plaintiff is punished for asserting his right. *Id.* Cases such as

U.S. v. Riley, 920 F.3d 200, 207 (4th Cir. 2019), where the question before the Court was the use of non-Mirandized statements in non-criminal proceedings, are even further afield.

The Government's second argument (at 25-26)—that Nur must plead that his devices have or will have contained information that will implicate him in a crime—is also false. *Marchetti v. U.S.*, 390 U.S. 39, 54 (1968), explains that the Fifth Amendment applies whenever the "hazards of incrimination" created by compulsion to testify "are not trifling or imaginary." Innocent people are as protected by the Fifth Amendment as the guilty. *See Reiner*, 532 U.S. at 21 ("one of the Fifth Amendment's basic functions is to protect innocent men who otherwise might be ensnared by ambiguous circumstances") (cleaned up) (emphasis original); *see also Slochower v. Board of Education*, 350 U.S. 551, 557 (1956) ("a witness may have a reasonable fear of prosecution and yet be innocent of any wrongdoing").

The Government's "Fourth" argument (at 27-28) also holds no water. The Government claims a border search exception to the Fifth Amendment. This exception does not exist. *U.S. v. FNU LNU*, 653 F.3d 144, 148 (2d Cir. 2011); *U.S. v. Pineda*, No. 09-cr-2542, 2010 WL 3034514, at *6 (D. Ariz. July 19, 2010) ("Fifth Amendment right to be free from self-incrimination does not cease to exist at the border") *report and recommendation adopted*, No. 09-cr-2542, 2010 WL 3038723 (Aug. 3, 2010). The only border exception to the Fifth Amendment involves the application of *Miranda* to routine questioning, *U.S. v. Lueck*, 678 F.2d 895, 899 (11th Cir. 1982); *see also U.S. v. Gupta*, 183 F.3d 615, 617 (7th Cir. 1999) (describing routine information as "identity, nationality, business, and claim of entitlement to enter"), and only when that questioning is not part of a custodial interrogation, *U.S. v. Adams*, 1 F.3d 1566, 1575 (11th Cir. 1993); *Gupta*, 183 F.3d at 617.

Even assuming the Government's search of Nur's devices are legal in the first place, the legality of the search does not justify violating the Fifth Amendment, even incidentally. *U.S. v. Hanon*, 428 F.2d 101, 105 (8th Cir. 1970) ("issue of the legality of the search under the Fourth Amendment is separate and distinct from the issue of whether the evidence seized is self-incriminating"); *Matter of Residence in Oakland,* 354 F. Supp. 3d at 1014 ("[e]ven if probable cause exists to seize devices located during a lawful search based on a reasonable belief that they belong to a suspect, probable cause does not permit the Government to compel a suspect to waive rights otherwise afforded by the Constitution, including the Fifth Amendment right against self-incrimination").

Finally, notwithstanding the Fifth Amendment violation, the Government asserts (at 27), adopting language from *U.S. v. McAuley*, 563 F. Supp. 2d 672, 678 (W.D. Tex. 2008), that a password is a "digital lock" that border agents can require opened like any other object. But *McAuley* and *U.S. v. Saboonchi* are Fourth Amendment cases involving forensic searches, not demands for passwords, and they at most stand for the proposition that forensic searches are allowed with reasonable suspicion. *See Saboonchi*, 990 F. Supp. 2d 536, 560 (D. Md. 2014) ("The court [in *McAuley*] also found that the existence of a password on the computer was no more relevant than the existence of a lock on a suitcase, neither of which automatically can convert a search from routine to nonroutine.").

The Government also suggests (at 27) that electronic devices are no different than luggage at a border, and the Government can require an individual to provide the passcode to a combination lock. But that is not right either. Unlike a phone, the Government has an absolute right to search luggage at the border. So if a person seeking entry at the border refuses to provide a lock passcode, the Government may break the lock, or it may declare the item

inadmissible. But the Government provides no citation for the support that it may punish someone for failure to provide the code.[4] *Compare with In re Grand Jury Subp. Duces Tecum Dated March 25, 2011*, 670 F.3d 1335, 1346 (11th Cir. 2012) ("[r]equiring Doe to use a decryption password is most certainly more akin to requiring the production of a combination" and therefore violates the Fifth Amendment); *see also Hubbell*, 530 U.S. at 43 indicating that *requiring production of a combination to a wall safe would be testimonial).

Of course, even if such a comparison otherwise supported the nonapplication of the Fifth Amendment in the luggage context, it would not apply here given *Kolsuz* and *Aigebekaen*, which explain the difference between ordinary luggage and digital devices.

* * *

The Government is right in one respect. This case is about the "Government's interest in preventing the entry of unwanted persons and effects." MTD at 27 (quoting *United States v. Flores-Montano*, 541 U.S. 149, 152 (2004)). Though the Government may wish it otherwise, Nur is an American citizen, not charged with any crime, who has an absolute right of entry into his country. And the Government does not appear to allege—and if it does, such allegation would be implausible—that the Government believes that there is anything on Nur's phone that would make it inadmissible contraband. Instead, the Government is attempting to use the happenstance of the border to perform an invasive investigation of an American

[4] Nur accepts that, ***if the Government has a constitutional right to perform a forensic search of an electronic device under the Fourth Amendment***, it may seize the device for the reasonably minimal time it requires to do the search. But that neither permits the Government to compel password testimony nor punish Nur—for instance, by threatening him, by performing additional, intrusive searches, or by unnecessarily prolonging his detention—as a punishment for his failure to waive his Fifth Amendment rights. Relatedly, the question of whether a Court may refuse to admit (and therefore permanently seize) a device it cannot adequately search by forensic means is not presented by this case.

citizen, despite having neither probable cause nor even reasonable suspicion that the American citizen is involved in either a particular crime or any crime at all. Neither the Fourth nor the Fifth Amendment of the Constitution permits the border to be used in this way.

CONCLUSION

The Court should deny the Government's Motion to Dismiss.

Respectfully submitted,

August 1, 2022

CAIR LEGAL DEFENSE FUND

BY: /s/ Lena F. Masri
Lena F. Masri (VA 93291)
lmasri@cair.com
Gadeir I. Abbas (VA 81161)
gabbas@cair.com
Justin M. Sadowsky (VA 73382)
jsadowsky@cair.com
453 New Jersey Ave., S.E.
Washington, DC 20003
Phone: (202) 742-6420
Fax: (202) 488-0833